CLAIMS

What is claimed is:

1. A method for controlling access to protected resources within a distributed data processing system, the method comprising:

receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

generating a response to the request;

refreshing the single-use token; and

sending the response and the refreshed single-use token to the client.

2. The method of claim 1 further comprising:

determining that the single-use token is a service token, wherein a service token is issued by the first server; and

refreshing the single-use service token at the first server.

3. The method of claim 1 wherein the session information in the single-use token is a session key.

4. The method of claim 1 further comprising:

determining that the single-use token is a domain token;

generating a client authorization credential request;

sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain.

5. The method of claim 4 further comprising:

validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server;

generating the client authorization credential;

refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server; and

sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server.

6. The method of claim 5 further comprising:

storing the client authorization credential at the first server;

generating a single-use service token associated with the client or the user of the client; and

sending to the client the single-use service token along with the response and the single-use domain token.

7. The method of claim 1 further comprising:

receiving a login request from the client at the second server;

challenging the client to provide authentication data;

receiving authentication data from the client;

authenticating the client;

generating a single-use domain token associated with the client or the user of the client;

generating an authentication response; and

sending the authentication response and the single-use domain token to the client.

8. The method of claim 7 further comprising:

determining that the login request is a redirected request from the first server; and

modifying the authentication response to redirect the client to the first server.

9. An apparatus for controlling access to protected resources within a distributed data processing system, the apparatus comprising:

means for receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

means for validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

means for generating a response to the request;

means for refreshing the single-use token; and

means for sending the response and the refreshed single-use token to the client.

10. The apparatus of claim 9 further comprising:

means for determining that the single-use token is a service token, wherein a service token is issued by the first server; and

means for refreshing the single-use service token at the first server.

11. The apparatus of claim 9 wherein the session information in the single-use token is a session key.

12. The apparatus of claim 9 further comprising:

means for determining that the single-use token is a domain token;

means for generating a client authorization credential request;

means for sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain.

13. The apparatus of claim 12 further comprising:

means for validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server;

means for generating the client authorization credential;

means for refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server; and

means for sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server.

14. The apparatus of claim 13 further comprising:

means for storing the client authorization credential at the first server;

means for generating a single-use service token associated with the client or the user of the client; and

means for sending to the client the single-use service token along with the response and the single-use domain token.

15. The apparatus of claim 9 further comprising:

means for receiving a login request from the client at the second server;

means for challenging the client to provide authentication data;

means for receiving authentication data from the client;

means for authenticating the client;

means for generating a single-use domain token associated with the client or the user of the client;

means for generating an authentication response; and

means for sending the authentication response and the single-use domain token to the client.

16. The apparatus of claim 15 further comprising:

means for determining that the login request is a redirected request from the first server; and

means for modifying the authentication response to redirect the client to the first server.

17. A computer program product on a computer readable medium for controlling access to protected resources within a distributed data processing system, the computer program product comprising:

instructions for receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

instructions for validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

instructions for generating a response to the request;

instructions for refreshing the single-use token; and

instructions for sending the response and the refreshed single-use token to the client.

18. The computer program product of claim 17 further comprising:

instructions for determining that the single-use token is a service token, wherein a service token is issued by the first server; and

instructions for refreshing the single-use service token at the first server.

19. The computer program product of claim 17 wherein the session information in the single-use token is a session key.

20. The computer program product of claim 17 further comprising:

instructions for determining that the single-use token is a domain token;

instructions for generating a client authorization credential request;

instructions for sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain.

21. The computer program product of claim 20 further comprising:

instructions for validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server;

instructions for generating the client authorization credential;

instructions for refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server; and

instructions for sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server.

22. The computer program product of claim 21 further comprising:

instructions for storing the client authorization credential at the first server;

instructions for generating a single-use service token associated with the client or the user of the client; and

instructions for sending to the client the single-use service token along with the response and the single-use domain token.

23. The computer program product of claim 17 further comprising:

instructions for receiving a login request from the client at the second server;

instructions for challenging the client to provide authentication data;

instructions for receiving authentication data from the client;

instructions for authenticating the client;

instructions for generating a single-use domain token associated with the client or the user of the client;

instructions for generating an authentication response; and

instructions for sending the authentication response and the single-use domain token to the client.

24. The computer program product of claim 23 further comprising:

instructions for determining that the login request is a redirected request from the first server; and

instructions for modifying the authentication response to redirect the client to the first server.